UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/664,613	09/17/2003	Sean J. Mullan	SUN03-06(P9621)	4049

7590 06/14/2007	EXAMINER
Barry W. Chapin, Esq.	CHAI, LONGBIT
CHAPIN & HUANG, L.L.C.	
Westborough Office Park	
1700 West Park Drive	
Westborough, MA 01581	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/664,613	MULLAN ET AL.
	Examiner	Art Unit	
	Longbit Chai	2131	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>02 May 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-4,6-20 and 22-34</u> is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ .Claim(s) <u>1-4,6-20 and 22-34</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>17 September 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Currently pending claims are 1 – 4, 6 – 20 and 22 – 34.

Response to Arguments

2.   Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3.   As per claim 1, 10, 29 and 32 – 34, Applicant asserts Kato does not teach "unencumbered by signature generation operability" (Remarks: Page 15, 1st Para). Examiner respectfully disagrees. Examiner notes the broadest and reasonable claim interpretations are made, according to MPEP 2111, for example, Kato teaches (a) no method or algorithm for embedding an XML signature S into the XML document D are required to be specified (Kato: Para [0084]), (b) The present invention is applicable to a future specification change without being limited to a specific version of XML-Signature (Kato: Para [0078] Last sentence) and (c) receiving a request for signifying the managed XML document from a client – i.e. the server signing the document for a client (Kato: Para [0025]) and as such Kato does teach the client is unencumbered by signature generation operability.

4.   Furthermore, Applicant asserts Kato does not teach "storing in a nondestructive manner because Kao teaches overwriting the signature element of the XML message" (Remarks: Page 15, 3rd Para). Examiner respectfully disagrees because Kato teaches the "signature template" can be replaced upon the completion of an XML signature – i.e. not the payload data to be stored, as recited in the claim, can be overwritten (Kato: Para [0088]).

5.   As per claim 20, 29, 32 – 34, Applicant asserts Kato does not teach "storing, in the signature portion, authentication indicators according to the predetermined protocol" (Remarks:

Page 16, 2nd Para). Examiner respectfully disagrees. Examiner notes the broadest and

reasonable claim interpretations are made, according to MPEP 2111, for example, Kato teaches

generating a structure of an XML signature S, generating an element of public key information

based on a Subject name of a public key certificate, and inserting the element into an XML

signature S (Kato: Para [0108]) where the element of public key information based on a Subject

name of a public key certificate stored in the signature portion can be broadly interpreted as an

<u>authentication indicator</u> according to the XML predetermined protocol.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by
another filed in the United States before the invention by the applicant for patent or (2) a patent
granted on an application for patent by another filed in the United States before the invention by the
applicant for patent, except that an international application filed under the treaty defined in section
351(a) shall have the effects for purposes of this subsection of an application filed in the United States
only if the international application designated the United States and was published under Article 21(2)
of such treaty in the English language.

6.   Claims 1 – 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Kato et al.

(U.S. Patent 2002/0040431).

As per claim 1, 10 and 20, Kato teaches a method for transmitting data according to a

signature-based protocol comprising:

generating, at a server (Kato : Para [0079]), a signature corresponding to a signature

block, the signature block having a covered data portion and an information object portion (Kato

: Para [0079] – [0081] and Para [108]: a signature template describes a series of "signature

target information", which is qualified as a covered data and the "digital content" is qualified as

an information object portion), the server conversant in a predetermined protocol and the

signature and signature block being conformant with the predetermined protocol (Kato : Para

[0003]: conforming to standard XML signature syntax / format and processing protocol);

storing the signature in the signature block (Kato : Para [0079]: XML Signature S is

considered as a part of the signature block, where signature value is stored at the s2);

transmitting to a client also conversant in the predetermined protocol (Kato : Para

[0030]), the signature block, the signature block further operable to store, in the information

object portion, payload data in a nondestructive manner, the nondestructive manner operable to

preserve the covered data portion and corresponding signature without regenerating the

signature (Kato : Para [0088] Last Sentence and Para [0080]: (a) the contents (i.e. digital

context) of the signed XML document Ds are generated after an XML signature (i.e. signature

template) is completed (b) each signature target information (i.e. covered data) can be

individually separate from the digital context – i.e. each signature only renders "local

significance" (Para [0080]) and thus not required to be regenerated (or affected) by the insertion

of any other digital context payload), storing in the information object portion further comprises

storing the payload data at a client, the client being unencumbered by signature generation

operability (Kato: Para [0084], [0078] and [0025]: Examiner notes the broadest and reasonable

claim interpretations are made, according to MPEP 2111, for example, Kato teaches (a) no

method or algorithm for embedding an XML signature S into the XML document D are required

to be specified (Kato: Para [0084]), (b) The present invention is applicable to a future

specification change without being limited to a specific version of XML-Signature (Kato: Para

[0078] Last sentence) and (c) receiving a request for signifying the managed XML document

from a client – i.e. the server signing the document for a client which is also interpreted as a

"non-signing client which does not compute the signature" (Kato: Para [0025])).

As per claim 29, Kato teaches method for transmitting data in a network system according to a signature based protocol comprising:

identifying, at a server, data adapted for cryptographic transmission (Kato : Para [0079]);

computing a digest on the identified data, the digest substantially indicative of the identified data (Kato : Para [0079] – [0081] and Para [108]: a hash (or summary value) is a digest value);

building, according to a cryptographic scripting language (Kato : Para [0003]: conforming to standard XML signature syntax / format and processing scripting language), a signature block, the signature block having a signed data portion, a signature value portion, a key information portion, and at least one information object portion (Kato : Para [0079] – [0081] and Para [108]: a signature template describes a series of "signature target information", which is qualified as a covered data and the "digital content" is qualified as an information object portion), the signature value portion operable to store the signature as an authentication indicator according to the predetermined protocol, further comprises storing the signature in the signature value portion (Kato: Para [0108]: Examiner notes the broadest and reasonable claim interpretations are made, according to MPEP 2111, for example, Kato teaches generating a structure of an XML signature S, generating an element of public key information based on a Subject name of a public key certificate, and inserting the element into an XML signature S – i.e. where the element of public key information based on a Subject name of a public key certificate stored in the signature portion can be broadly interpreted as an authentication indicator according to the XML predetermined protocol);

storing the identified data in the signed data portion of a signature block (Kato : Para [0079] – [0081] and Para [108]: the signature target information is the identified data portion);

retrieving, from a public key infrastructure (PKI) a public and private key pair operable for cryptographic operations (Kato : Para [0081] – [0082]);

generating, at a server, a signature value from the private key corresponding to the computed digest, the signature substantially unrecreatable by data other than the computed digest (Kato : Para [0081] – [0082]);

storing the signature value in the signature value portion of the signature block;

storing the public key corresponding to the private key in the key information portion to provide a self-authenticating transmission (Kato : Para [0079] – [0082]), the signature value portion and corresponding signature value persisting as a signature block according to the predetermined protocol including the payload data portion (Kato: Para [0252]: the signature block with the signature template Dt and the included content of the XML document is the payload data portion according to the XML predetermined protocol);

transmitting, according to the predetermined protocol, the signature block to a client (Kato : Para [0030]) also conversant in the scripting language and operable to store payload data in the information object portion independently of the signature value portion (Kato : Para [0088] Last Sentence and Para [0080]: (a) the contents (i.e. digital context) of the signed XML document Ds are generated after an XML signature (i.e. signature template) is completed (b) each signature target information (i.e. covered data) can be individually separate from the digital context – i.e. each signature only renders "local significance" (Para [0080]) and thus not required to be regenerated (or affected) by the insertion of any other digital context payload), storing in the information object portion further comprises storing the payload data at a client, the client being unencumbered by signature generation operability (Kato: Para [0084], [0078] and [0025]: Examiner notes the broadest and reasonable claim interpretations are made, according to MPEP 2111, for example, Kato teaches (a) no method or algorithm for embedding

an XML signature S into the XML document D are required to be specified (Kato: Para [0084]),

(b) The present invention is applicable to a future specification change without being limited to a

specific version of XML-Signature (Kato: Para [0078] Last sentence) and (c) receiving a request

for signifying the managed XML document from a client – i.e. the server signing the document

for a client (Kato: Para [0025])).

As per claim 32 – 34, Kato teaches a method for transmitting data from a nonsignine

client according to a signature based protocol (Kato : Para [0079]: a nonsigning client is

interpreted as the client that requires and requests the signature capability from a server with

respect to XML signature), comprising:

receiving a signature block and a signature corresponding to the signature block, the

signature block having a covered data portion corresponding to the signature, and an

information object portion, the receiving client conversant in a predetermined protocol and the

signature and signature block being conformant with the predetermined protocol (Kato : Para

[0003] and Para [0030]: (a) conforming to standard XML signature syntax / format and

processing scripting language (b) transmitting from a server to a client – i.e. received at the

client), a signature block, the signature block having a signed data portion, a signature value

portion, a key information portion, and at least one information object portion (Kato : Para [0079]

– [0081] and Para [108]: a signature template describes a series of "signature target

information", which is qualified as a covered data and the "digital content" is qualified as an

information object portion;

storing, in the information object portion of the signature block, payload data in a

nondestructive manner, the nondestructive manner operable to preserve the covered data

portion and the corresponding signature without regenerating the signature (Kato : Para [0088]

Last Sentence and Para [0080]: (a) the contents (i.e. digital context) of the signed XML

document Ds are generated after an XML signature (i.e. signature template) is completed (b)

each signature target information (i.e. covered data) can be individually separate from the digital

context – i.e. each signature only renders "local significance" (Para [0080]) and thus not

required to be regenerated (or affected) by the insertion of any other digital context payload),

wherein storing in the information object portion further comprises storing the payload data at a

client, the client being unencumbered by signature generation operability (Kato: Para [0084],

[0078] and [0025]: Examiner notes the broadest and reasonable claim interpretations are made,

according to MPEP 2111, for example, Kato teaches (a) no method or algorithm for embedding

an XML signature S into the XML document D are required to be specified (Kato: Para [0084]),

(b) The present invention is applicable to a future specification change without being limited to a

specific version of XML-Signature (Kato: Para [0078] Last sentence) and (c) receiving a request

for signifying the managed XML document from a client – i.e. the server signing the document

for a client (Kato: Para [0025])).

        transmitting, according to the predetermined protocol, the signature block to a recipient

destination conversant in the predetermined protocol, the information object portion included in

the signature block according to the predetermined protocol (Kato : Para [0066]: the application

destination is qualified as a recipient destination, which is conversant in the predetermined XML

signature protocol), wherein the signature value portion operable to store the signature as an

authentication indicator according to the predetermined protocol, further comprises storing the

signature in the signature value portion (Kato: Para [0108]: Examiner notes the broadest and

reasonable claim interpretations are made, according to MPEP 2111, for example, Kato teaches

generating a structure of an XML signature S, generating an element of public key information

based on a Subject name of a public key certificate, and inserting the element into an XML

signature S – i.e. where the element of public key information based on a Subject name of a

public key certificate stored in the signature portion can be broadly interpreted as an

authentication indicator according to the XML predetermined protocol).

As per claim 2 and 11, Kato teaches the signature block further includes a signature

value portion, the signature value portion operable to store the signature as an authentication

indicator according to the predetermined protocol, wherein storing further comprises storing the

signature in the signature value portion (Kato : Para [0079] – [0081] and Para [108]).

As per claim 3, 12 and 22, Kato teaches the signature block further includes a key

information portion, further comprising storing an authentication indicator to a validation

instrument in the key information portion, the validation instrument operable to authenticate the

signature value portion using the signature (Kato : Para [0081] – [0082]).

As per claim 4 and 23, Kato teaches the validation instrument corresponds to an inverse

operation of the generating of the signature (Kato : Para [0081] – [0082]).

As per claim 24, Kato teaches storing in the information object portion further comprises

storing the payload data at a client, the client being unencumbered by signature generation

operability (Kato: Para [0084], [0078] and [0025]: Examiner notes the broadest and reasonable

claim interpretations are made, according to MPEP 2111, for example, Kato teaches (a) no

method or algorithm for embedding an XML signature S into the XML document D are required

to be specified (Kato: Para [0084]), (b) The present invention is applicable to a future

specification change without being limited to a specific version of XML-Signature (Kato: Para

[0078] Last sentence) and (c) receiving a request for signifying the managed XML document from a client).

As per claim 6 and 25, Kato teaches storing the payload data further comprises generating a transmission block conformant with the predetermined protocol and operable to be received as a signature authenticated transmission by a destination node according to the predetermined protocol (Kato : Para [0066]: the application destination is qualified as a recipient destination, which is conversant in the predetermined XML signature protocol).

As per claim 7 and 26, Kato teaches generating the signature further comprises generating a signature corresponding to the covered data portion of the signature block (Kato : Para [0079] – [0080]).

As per claim 8 and 27, Kato teaches computing a digest on the covered data portion, the digest substantially indicative of the data in the covered data portion (Kato : Para [0079] – [0081] and Para [108]: a hash (or summary value) is a digest value).

As per claim 9 and 28, Kato teaches the validation instrument is a public key and generating the signature further comprises generating a signature using the private key corresponding to the public key (Kato : Para [0081] – [0082]).

As per claim 13, Kato teaches the receiving is performed by a nonsigning client which does not compute the signature and is unencumbered by components operable to compute the

signature (Kato : Para [0079]: a nonsigning client is interpreted as the client that requires and requests the signature capability from a server).

As per claim 14, Kato teaches indexing a remote signature repository, and the client is further operable to store the received signature in the signature block according to the predetermined protocol (Kato : Para [0018] Line 10).

As per claim 15, Kato teaches receiving an authentication instrument corresponding to the signature, and storing the received authentication instrument in the signature block with the signed information portion and the signature (Kato : Para [0082] and Para [0079]).

As per claim 16, Kato teaches the received authentication instrument is a public key corresponding to the private key for generating the signature, and storing further comprising forming a self-signed message by storing the public key in the key information portion (Kato : Para [0082] and Para [0079]: the public key is stored in the XML signature block S corresponding to the private key used to generate the signature value for authenticating and/or decrypting the signed info, which is equivalent to self-authenticating message (or a self-signed message), according to the instant specification (SPEC: Page 15 Line 4 – 7)).

As per claim 17, Kato teaches at the nonsigning client (Kato : Para [0079]: a nonsigning client is interpreted as the client that requires and requests the signature capability from a server), a plurality of signatures and corresponding covered data portions (Kato : Para [0080]); selecting a first signature for inclusion in a first signature message for transmission to a destination recipient; selecting a second signature different than the first signature for inclusion

in a second signature message for transmission to the same destination recipient (Kato : Para [0066] and Para [0080]: (a) a destination application is qualified as a destination recipient (b) more than one signature target information can be included in the same XML signature block S).

As per claim 18, Kato teaches selecting the first and second signatures is performed based on signature selection logic, the signature selection logic for analyzing the covered data portion and the information object portion of the signature message to select an expected signature result at the destination recipient (Kato : Para [0079] and Para [0080]: the selected covered data portion is the selected signature target information with respect to the associated digital content).

As per claim 19, Kato teaches the signature selection logic is operable for analyzing the covered data portion based on at least one of the content type, size, creation date, and sparsity of the data (Kato : Para [0079] and Para [0080]: the selected covered data portion is the selected signature target information with respect to the associated digital content, which is qualified as sparsity of the data – i.e. not the entire payload data content).

As per claim 30, Kato teaches the scripting language is operable to incorporate signature components such that the scripting language is operable with signing capability when signature components are available and operable without signing capability when signature components are unavailable, further comprising:

identifying the signature value portion from a subset of available fields in the signature block, the signature value corresponding to the identified subset and the remaining available fields independent of the signature value (Kato : Para [0079] – [0081] and Para [108]);

identifying, from the remaining available fields, payload data portions operable for

subsequent storage of data independent of the signature value and the signature value portion,

the payload data portions operable to be modified by subsequent recipients, wherein the

signature value portion and corresponding signature value persist as a signature block

according to the predetermined protocol including the payload data portions (Kato : Para [0088]

Last Sentence and Para [0080]: (a) the contents (i.e. digital context) of the signed XML

document Ds are generated after an XML signature (i.e. signature template) is completed (b)

each signature target information (i.e. covered data) can be individually separate from the digital

context – i.e. each signature only renders "local significance" (Para [0080]) and thus not

required to be regenerated (or affected) by the insertion of any other digital context payload).

As per claim 31, Kato teaches a system for signature use by a nonsigning client

generating, at a server (Kato : Para [0079]: a nonsigning client is interpreted as the client that

requires and requests the signature capability from a server), , the nonsigning client

unencumbered from cryptographic operation components, comprising:

at the client, identifying payload data adapted for storage in the information object

portions according to the scripting language independent of the signature value; and storing the

identified payload data in the information object portions in a nondestructive manner, the

nondestructive manner operable to preserve the covered data portion and corresponding

signature without regenerating the signature, the client unencumbered and inoperable to

encrypt and decrypt the signed data (Kato : Para [0088] Last Sentence and Para [0080]: (a) the

contents (i.e. digital context) of the signed XML document Ds are generated after an XML

signature (i.e. signature template) is completed (b) each signature target information (i.e.

covered data) can be individually separate from the digital context – i.e. each signature only

renders "local significance" (Para [0080]) and thus not required to be regenerated (or affected)

by the insertion of any other digital context payload).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as

set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date

of this final action.

Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner

can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100